# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-078555

(43)Date of publication of application : 14.03.2000

(51)Int.Cl. H04N 7/16
H04H 1/02
H04L 12/14

(21)Application number : 10-243906

(22)Date of filing : 28.08.1998

(71)Applicant : SONY CORP

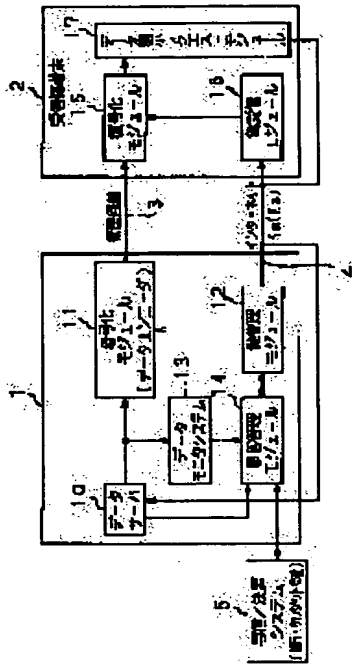
(72)Inventor : KUBOTA ICHIRO

## (54) CHARGING METHOD AND DEVICE FOR DATA TRANSMISSION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize charging for a data unit or a data class and for each contractor while keeping confidentiality of the data in the case of using a high speed data channel with a large capacity such as a digital CATV channel or a satellite broadcast to conduct a data service.

SOLUTION: The device has an encryption module that encodes data and serves encrypted data and a key management module 12 that manages an encryption key to decode the encrypted data and the distribution of the encryption key, and the device transmits the encrypted data to a receiver side terminal 2 via a satellite circuit 3 and transmits the encryption key to the receiver side terminal 2 via the Internet 4. A customer management module 14 manages charging of data received by the receiver side terminal 2 depending on a distribution form of the encrypted key transmitted from the key management module 12 to the receiver side terminal 2.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－78555
（P2000－78555A）
(43)公開日　平成12年３月14日(2000.3.14)

| (51)Int.Cl.' | 識別記号 | ＦＩ | | テーマコード'（参考） |
|---|---|---|---|---|
| Ｈ０４Ｎ　7/16 | | Ｈ０４Ｎ | 7/16 | Ｃ |
| Ｈ０４Ｈ　1/02 | | Ｈ０４Ｈ | 1/02 | Ｅ |
| Ｈ０４Ｌ　12/14 | | Ｈ０４Ｌ | 11/02 | Ｆ |

審査請求　未請求　請求項の数18　ＯＬ　（全 18 頁）

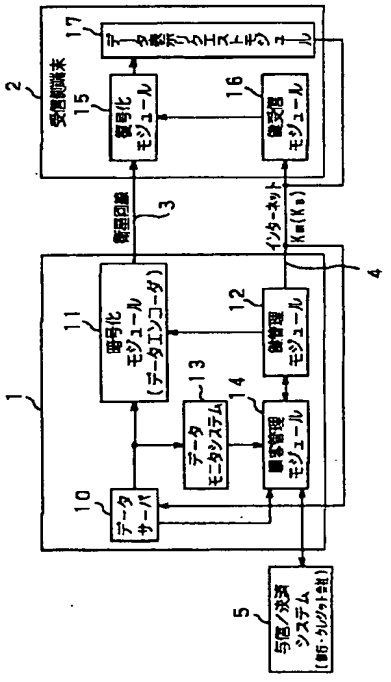
(21)出願番号　特願平10－243906

(22)出願日　平成10年８月28日(1998.8.28)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　窪田　一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100067736
弁理士　小池　晃　（外２名）

(54)【発明の名称】　データ伝送システムの課金方法及び装置

(57)【要約】
【課題】　衛星放送やディジタルＣＡＴＶ回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合に、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現する。
【解決手段】　データを暗号化して提供する暗号化モジュール１１と、暗号化されたデータの当該暗号化を解くための暗号鍵の管理及びその暗号鍵の配信を管理する鍵管理モジュール１２とを有し、暗号化したデータは衛星回線３を介して受信側端末２に送信し、暗号鍵はインターネット４を介して受信側端末に送信する。受信側端末２にて受信したデータに対する課金は、顧客管理モジュール１４が、鍵管理モジュール１２から受信側端末２に送信された暗号鍵の配信形態に応じて管理する。



1

【特許請求の範囲】
【請求項１】　通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法において、
上記データを暗号化して提供し、
上記暗号化されたデータの当該暗号化を解くための暗号鍵を管理し、
上記暗号鍵を配信し、
上記暗号鍵の配信形態に応じて上記課金を管理することを特徴とするデータ伝送システムの課金方法。
【請求項２】　少なくとも通信路が確立される毎に上記暗号鍵を配信することを特徴とする請求項１記載のデータ伝送システムの課金方法。
【請求項３】　少なくとも通信路が確立されている時間中に定期的に上記暗号鍵を配信することを特徴とする請求項１記載のデータ伝送システムの課金方法。
【請求項４】　上記暗号鍵の配信回数を管理し、
当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項２記載のデータ伝送システムの課金方法。
【請求項５】　上記暗号鍵の配信回数を管理し、
当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項３記載のデータ伝送システムの課金方法。
【請求項６】　通信路が確立されている接続時間を計測し、
当該接続時間に応じて課金を管理することを特徴とする請求項１記載のデータ伝送システムの課金方法。
【請求項７】　各通信路毎のデータ伝送量を計測し、
当該データ伝送量の総和に応じて課金を管理することを特徴とする請求項１記載のデータ伝送システムの課金方法。
【請求項８】　伝送するデータ種別により上記暗号鍵を対応させ、
当該データ種別による暗号鍵に応じて課金を管理することを特徴とする請求項１記載のデータ伝送システムの課金方法。
【請求項９】　上記通信回線は高速の第１のデータ伝送路と、当該第１のデータ伝送路よりも低速の第２のデータ伝送路とからなり、
上記第１のデータ伝送路にて上記暗号化されたデータを伝送し、
上記第２のデータ伝送路にて上記暗号鍵を伝送することを特徴とする請求項１記載のデータ伝送システムの課金方法。
【請求項１０】　通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金装置において、
上記データを暗号化して提供するデータ提供手段と、
上記暗号化されたデータの当該暗号化を解くための暗号鍵の管理及びその暗号鍵の配信を管理する鍵管理手段と、

2

上記暗号鍵の配信形態に応じて上記課金を管理する課金管理手段とを有することを特徴とするデータ伝送システムの課金装置。
【請求項１１】　上記鍵管理手段は、少なくとも通信路が確立される毎に上記暗号鍵を配信することを特徴とする請求項１０記載のデータ伝送システムの課金装置。
【請求項１２】　上記鍵管理手段は、少なくとも通信路が確立されている時間中に定期的に上記暗号鍵を配信することを特徴とする請求項１０記載のデータ伝送システムの課金装置。
【請求項１３】　上記鍵管理手段は、上記暗号鍵の配信回数を管理し、
上記課金管理手段は、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項１１記載のデータ伝送システムの課金装置。
【請求項１４】　上記鍵管理手段は、上記暗号鍵の配信回数を管理し、
上記課金管理手段は、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項１２記載のデータ伝送システムの課金装置。
【請求項１５】　通信路が確立されている接続時間を計測する接続時間計測手段を備え、
上記課金管理手段は、当該接続時間に応じて課金を管理することを特徴とする請求項１０記載のデータ伝送システムの課金装置。
【請求項１６】　各通信路毎のデータ伝送量を計測するデータ伝送量計測手段を備え、
上記課金管理手段は、当該データ伝送量の総和に応じて課金を管理することを特徴とする請求項１記載のデータ伝送システムの課金装置。
【請求項１７】　上記鍵管理手段は、伝送するデータ種別により上記暗号鍵を対応させ、
上記課金管理手段は、当該データ種別による暗号鍵に応じて課金を管理することを特徴とする請求項１０記載のデータ伝送システムの課金装置。
【請求項１８】　上記通信回線は高速の第１のデータ伝送路と、当該第１のデータ伝送路よりも低速の第２のデータ伝送路とからなり、
上記データ提供手段は、上記暗号化されたデータを上記第１のデータ伝送路に伝送し、
上記鍵管理手段は、上記暗号鍵を上記第２のデータ伝送路に伝送することを特徴とする請求項１０記載のデータ伝送システムの課金装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法及び装置に関する。

3

【０００２】
【従来の技術】衛星放送やディジタルケーブルテレビジョン（以下、ＣＡＴＶと記す）回線のような大容量のデータ回線を使用してデータサービスを行う場合には、先行しているディジタルオーディオ／ビデオサービスで用いられているトランスポートストリーム（Transport Stream、以下ＴＳと記す）パケットにインターネットプロトコル（Internet Protocol、以下ＩＰと記す）等のデータパケットを重畳させ、データサービスを行う事が一般的である。
【０００３】従って、データサービスの顧客管理を行う上で一番簡単な方法としては、ＴＳ毎のスクランブルを行うＩＣカードによる限定アクセス機能（Conditional Access、以下適宜ＣＡと記す）を用いる方法が挙げられる。この場合、ＴＳ毎のスクランブルには、ＴＳパケットのパケットＩＤ（Packet IDentification、以下ＰＩＤと記す）によって識別される特定の暗号化キーを用いた、マルチプレクサによるスクランブル処理が行われる。
【０００４】例えばインターネットサービスシステムの場合は、送出側において、ある帯域を占有する一つのエンコーダが、サービス（チャンネル）として定義される特定のＰＩＤを持つＴＳパケットを生成し、このＴＳパケットの中に、複数ユーザのパーソナルコンピュータ（ＰＣ）へのＩＰデータグラムが多重される。
【０００５】ＩＣカードによるＣＡ機器を用いた場合、ユーザグループ（例えば一つの企業）と他のユーザグループの間では、それぞれエンコーダが異なり、違ったスクランブル鍵を持つため、当該スクランブル鍵が破られない限り、互いに相手のデータを盗み見る事は不可能である。
【０００６】一方、グループ内では、既にスクランブルが解かれたデータを受信可能であるため、不正に他人のデータを盗み見る事が可能である。但し、ユーザグループが一企業であり、専用線的な使い方をする場合は、特にデータの不正読み出しについて注意を払う必要が無い。
【０００７】
【発明が解決しようとする課題】しかしながら、一つのサービス（チャンネル）を利用して不特定多数のユーザに対してデータサービスを提供するような時には、この点が問題となる。すなわち、一般のホームページのような、誰でもアクセス可能なデータについては他人に見られても問題は無いと思われるが、いわゆるＳＯＨＯ（Small Office HomeOffice）のユーザのように、仕事上秘密性の高いデータのやりとりを行う場合には、データを他人に見られる事は非常に問題となり、したがってデータの秘密性を保つ為の手段が必要となる。
【０００８】また、衛星放送やディジタルＣＡＴＶ回線等を使用したデータサービスを行う場合、ユーザに提供

4

したデータに対する課金のシステムを構築しなければならない。衛星ディジタル放送では、ＩＣカードによる課金システムが既に構築されているが、このＩＣカードによる課金システムは、元々オーディオ及びビデオ放送の番組単位の課金を基本としたシステムであり、データ単位やデータ種別毎の課金には必ずしも適していない。
【０００９】そこで、本発明はこのような状況に鑑みてなされたものであり、衛星放送やディジタルＣＡＴＶ回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合において、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現する、データ伝送システムの課金方法及び装置を提供することを目的とする。
【００１０】
【課題を解決するための手段】本発明のデータ伝送システムの課金方法及び装置は、通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法であり、データを暗号化して提供し、その暗号化されたデータの当該暗号化を解くための暗号鍵を管理してその暗号鍵を配信すると共に、そのときの暗号鍵の配信形態に応じて課金を管理することにより、上述した課題を解決する。
【００１１】
【発明の実施の形態】本発明の好ましい実施の形態について、図面を参照しながら説明する。
【００１２】以下、本発明にかかるデータ伝送システムの課金方法及び装置が適用される一実施の形態であるデータサービスシステムの全体構成について、図１を用いて説明する。
【００１３】図１に示すデータサービスシステムにおいて、データ送信装置１のデータサーバ１０は、例えばオーディオデータやビデオデータ等だけでなく、コンピュータプログラム等の各種データをディジタルコンテンツとして格納してなるものである。本実施の形態では、特にデータサービスを例に挙げているため、当該データサーバ１０から取り出されるディジタルコンテンツをコンピュータプログラム等の各種データ（以下、単にデータとする）として説明する。このデータサーバ１０から出力されたデータは、暗号化モジュール１１に送られる。
【００１４】暗号化モジュール（データエンコーダ）１１は、鍵管理モジュール１２から送られてきた暗号鍵を用いて、上記データサーバ１０からのデータを暗号化し、当該暗号化データを、例えば衛星回線やディジタルＣＡＴＶ回線等の大容量且つ高速の通信回線に送信（配信）する。
【００１５】ここで、本実施の形態では、通信回線として衛星ディジタル放送に使用される衛星回線３を用いた場合を例に挙げている。したがって当該暗号化モジュール１１では、上記データサーバ１０からのデータをＩＰ（Internet Protocol）等のデータパケットにパケット

化（すなわちＩＰデータグラムを生成）して暗号化し、この暗号化データ（以下、セクションデータとする）に所定の付加情報（例えばＭＡＣ（Media Access Control）アドレスを含むヘッダ等）を付加したデータを、ディジタルオーディオ／ビデオサービスで用いられているようなＴＳ（Transport Stream）パケットに重畳させ、当該ＴＳパケットを衛星回線３に送信（すなわち配信）するようにしている。なお、このデータサーバ１０におけるＩＰデータグラムの生成及び暗号化モジュール１１における暗号化処理（セクションデータの生成処理）の詳細及び具体的構成、当該セクションデータ及びそのヘッダに含まれるＭＡＣアドレス等の詳細については後述する。

【００１６】鍵管理モジュール１２は、上記暗号化モジュール１１におけるＩＰデータグラムの暗号化に使用する暗号鍵を管理する。この鍵管理モジュール１２からの暗号鍵は、電話回線やＩＳＤＮ（Integrated Services Digital Network：統合サービスディジタル通信網）等を使用した地上回線を介して伝送される。本実施の形態では、当該地上回線として、電話回線やＩＳＤＮ等を使用したインターネット４を例に挙げている。上記鍵管理モジュール１２がインターネット４を介して受信側端末１７に送信する暗号鍵は、セキュリティ確保のため当然暗号化されているものとする。当該鍵管理モジュール１２が管理する暗号鍵、及びこの暗号鍵の送信並びに暗号化等の詳細については後述する。

【００１７】受信側端末１７の鍵受信モジュール１６は、上記インターネット４を介して送信されてきた上記暗号鍵を受信して復号（暗号解読）し、当該受信及び復号した暗号鍵を受信側端末１７内の復号化モジュール１５に転送する。

【００１８】復号化モジュール１５は、上記衛星回線３を介して受信したデータのＴＳパケットから前記セクションデータを取り出し、当該セクションデータのヘッダに含まれるＭＡＣ（Media Access Control）アドレスに基づいて、対応する暗号鍵を鍵受信モジュール１６から受け取り、当該暗号鍵を用いて上記セクションデータ内の暗号化されたＩＰデータグラムの暗号解読（データデコード）を行う。なお、当該復号化モジュール１５における暗号解読の詳細については後述する。

【００１９】データ表示リクエストモジュール１７は、提供を受けたいデータのリクエストを、例えばインターネット４を通じてデータ送信装置１に送信し、また、必要に応じて表示を行う。

【００２０】データ送信装置１のデータモニタシステム１３は、個々の契約者の受信側端末２に対して送信（配信）されるデータ量（情報量）や通信路が確立された接続時間などをモニタする。例えば送信されるデータ量をモニタする場合には、送信されるデータのアドレス毎のデータ量或いはパケット毎のデータ量を集計し、また、



接続時間をモニタする場合には、図示しない内部時計からの時間情報に基づいて当該接続時間を集計する。

【００２１】また、データ送信装置１の顧客管理モジュール１４は、上記鍵管理モジュール１２に対して指令を行い、当該鍵管理モジュール１２による暗号鍵の配信をどのように行うかを管理する。また、顧客管理モジュール１４は、契約者毎の契約形態やデータ単位毎或いはデータ種別毎の課金形態によって様々な課金方法の管理を行うと共に、それら契約形態や課金方法に基づいて契約者毎の課金情報の集計及び管理を行う。さらに、顧客管理モジュール１４は、金融／クレジット会社等の与信／決済システム５と回線が繋がっており、したがって、当該顧客管理モジュール１４は、当該与信／決済システム１７を通して、上記集計された課金情報に基づいた個々の契約者への請求書の発行及び入金管理等を行う。

【００２２】ここで、本実施の形態のようなデータサービスシステムにおける契約者の契約形態としては、以下の３種類の契約形態（第１～第３の契約形態）が考えられる。

【００２３】「第１の契約形態」データサービスを受ける事が可能な契約を一旦行えば、受信するデータ種別／データ量にかかわらず、一定の課金がなされる契約形態（フラット／定額制課金）。

【００２４】「第２の契約形態」受信するデータ量によって課金される契約形態（従量制課金）。

【００２５】「第３の契約形態」受信するデータ種別によって課金される契約形態（コンテンツ課金）。

【００２６】このため、上記顧客管理モジュール１４は、データサービスにおいて契約者によりなされる課金設定により、上記第１～第３までの契約形態のうち何れか一つを選択する。

【００２７】先ず、上記第１の契約形態（フラット／定額制課金）にて契約がなされた場合、契約者（受信側端末２）は、暗号鍵を一旦受け取った後はそのまま当該暗号鍵を更新する事無く、ずっと使える事になり、最も簡単且つ便利である。

【００２８】この第１の契約形態にて契約がなされた場合の課金は、例えば毎月一定額の課金等が考えられ、したがって、上記顧客管理モジュール１４では、当該第１の契約形態を選択した契約者に対しては当該毎月一定額となるような課金を、上記与信／決済システム１７を通して行う。なお、当該第１の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【００２９】ただし、暗号鍵を変更せずに常に同一の暗号鍵を使用していると、例えばハッカー等によって暗号鍵が解明される恐れがある為、一般にはあるタイミングで暗号鍵を変更する必要がある。

【００３０】上記暗号鍵を変更するタイミングとしては、以下の３種類の変更タイミング（第１～第３の暗号

鍵変更タイミング）が考えられる。

【００３１】「第１の暗号鍵変更タイミング」暗号鍵の不正解読等の問題が発生するまで暗号鍵の変更を行わない。言い換えれば、問題が発生したタイミングで暗号鍵を変更する。

【００３２】「第２の暗号鍵変更タイミング」通信路（セッション）が確立される毎に暗号鍵を配信する。すなわち、通信路が確立される毎のタイミングで異なる暗号鍵を配信する。

【００３３】「第３の暗号鍵変更タイミング」通信路（セッション）が確立されて通信を行っている時間中は定期的に暗号鍵の配信を行う。すなわち、通信路が確立されて通信を行っている時間中の定期的なタイミングで異なる暗号鍵を配信する。

【００３４】これら３つの暗号鍵変更タイミングは第１の暗号鍵変更タイミングから順にセキュリティ性が高くなっており、システムへのセキュリティへの要求度によってどの変更タイミングを取るかを決定すれば良い。

【００３５】次に、上記第２の契約形態（従量制課金）にて契約がなされた場合、すなわち、受信するデータ量によって課金を行う場合は、契約者（受信側端末２）が受信したデータ量（言い換えればデータ送信装置１が送信したデータ量）を計測しなければならない。このデータ量の計測方法としては、以下の３種類の計測方法（第１～第３のデータ量計測方法）が考えられる。

【００３６】「第１のデータ量計測方法」通信路（セッション）が確立されて通信を行っている時間中は定期的に暗号鍵の配信を行う上記第３の暗号鍵変更タイミングの場合において、通信路（セッション）が確立されている期間中に配信される暗号鍵の配信回数を数え、この配信回数からデータ量を計測する。

【００３７】「第２のデータ量計測方法」通信路（セッション）が確立されている期間の接続時間を計り、この接続時間からデータ量を計測する。

【００３８】「第３のデータ量計測方法」各通信路（セッション）毎の実際のデータ伝送量を計測する。例えば送信されるアドレス毎或いはパケット数からデータ量を計測する。

【００３９】したがって、この第２の契約形態（従量制課金）にて契約がなされた場合の課金は、上記第１～第３のデータ量計測方法の何れを選択したかにより異なる。すなわち、第２の契約形態（従量制課金）にて契約がなされた場合の課金方法としては、上記第１～第３のデータ量計測方法に対応した以下の３種類の課金方法（第１～第３の課金方法）が考えられる。なお、当該第２の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【００４０】「第１の課金方法」上記第１のデータ量計測方法のように、通信路（セッション）の確立された期間中に配信された暗号鍵の配信回数からデータ量を計測した場合は、当該暗号鍵の配信回数に応じて契約者への課金を行う。すなわち、この第１の課金方法の場合の上記顧客管理モジュール１４では、通信路（セッション）の確立された期間中に鍵管理モジュール１２が受信側端末２に配信した暗号鍵の配信回数を管理し、この配信回数に応じた課金を、上記与信／決済システム１７を通して行う。



【００４１】「第２の課金方法」上記第２のデータ量計測方法のように、通信路（セッション）の確立された期間中の接続時間を計ってデータ量を計測した場合は、当該接続時間に応じて契約者への課金を行う。すなわち、この第２の課金方法の場合の上記顧客管理モジュール１４では、通信路（セッション）の確立された期間中にデータモニタシステム１３が集計した接続時間を管理し、この接続時間に応じた課金を、上記与信／決済システム１７を通して行う。

【００４２】「第３の計測課金方法」上記第３のデータ量計測方法のように、各通信路（セッション）毎のデータ伝送量を直接計測した場合は、当該データ伝送量の総和に応じて契約者への課金を行う。すなわち、この第３の課金方法の場合の上記顧客管理モジュール１４では、通信路（セッション）の確立された期間中にデータモニタシステム１３が集計したデータ伝送量を管理し、このデータ伝送量の総和に応じた課金を、上記与信／決済システム１７を通して行う。

【００４３】次に、上記第３の契約形態（コンテンツ課金）にて契約がなされた場合は、受信するデータ種別（コンテンツ）によって課金を行う。すなわち、契約者（受信側端末２）に送信されるコンテンツはそれぞれコンテンツ毎に異なった暗号鍵により暗号化されているため、そのコンテンツを暗号化したときの暗号鍵は予めリクエストの有った契約者（受信側端末２）にのみ配信され、当該暗号鍵を受け取った契約者（受信側端末２）だけが上記暗号化されたコンテンツを正しく復号し、データを取り出すことができるようになされている。このため、当該第３の契約形態のように、受信するデータ種別（コンテンツ）によって課金を行う場合は、契約者（受信側端末２）に受信した暗号鍵（暗号化されたコンテンツの暗号解読を行うための暗号鍵）に応じた課金、言い換えれば契約者（受信側端末２）に対して送信した暗号鍵に応じた課金を行う。なお、この第３の契約形態の場合、課金される金額は、データ種別すなわちコンテンツに応じて異なる額としたり、データの重要度に応じて異なる額とすることも可能である。言い換えれば、契約者（受信側端末２）に送った暗号鍵の種類によって、課金の額を変更することができる。

【００４４】したがって、この第３の契約形態の場合の上記顧客管理モジュール１４では、鍵管理モジュール１２が契約者（受信側端末２）に対して送信した暗号鍵に応じた課金を、上記与信／決済システム１７を通して行

う。なお、当該第３の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【００４５】次に、上述したような第１～第２の契約形態にて契約がなされた場合において、課金のための図１の顧客管理モジュール１４の具体的構成及び動作について、図２を参照しながら説明する。

【００４６】この図２において、顧客管理モジュール１４は、個々の契約者毎の契約形態（前記第１～第３の契約形態）及び前記第１～第３の暗号鍵変更タイミング、第１～第３のデータ量計測方法、第１～第３の課金方法についての各情報を顧客情報として格納する顧客データベース２１を有すると共に、個々のデータ種別毎のコンテンツリストを格納して個々のデータ種別毎にその情報量を管理するコンテンツ管理サーバ２０を有している。

【００４７】先ず最初に、前記第１の契約形態（フラット／定額制課金）の場合の顧客管理モジュール１４における課金処理の流れについて説明する。

【００４８】契約者（受信側端末２）から通信路（セッション）確立の要求（リクエスト）がインターネット４等の地上回線を経由してなされた場合、このリクエストは一旦、鍵管理モジュール１２に転送される。当該リクエストを受け取った鍵管理モジュール１２は、顧客管理モジュール１４の顧客認証／鍵管理モジュール制御部２３に対して、暗号鍵の配信要求を行う。

【００４９】顧客認証／鍵管理モジュール制御部２３は、顧客データベース２１に格納した顧客情報を用いて、このリクエストを行った契約者の契約情報をチェックし、暗号鍵を与えて良いか否かを判断し、与えて良いと判断された場合は、その顧客情報に記述された鍵配信の形態と合わせて、暗号鍵の配信を鍵管理モジュール１２に指示する。また同時に、顧客認証／鍵管理モジュール制御部２３は、利用履歴ログ収集部２４に対して当該リクエストを行った契約者（受信側端末２）の利用履歴を登録し、利用料課金処理部２５に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、さらに請求・収納・支払・滞納管理部２６を介して銀行やクレジット会社等の与信／決済システム５に対して契約者への請求書の発行依頼等を行う。

【００５０】次に、前記第２の契約形態（従量制課金）を行う場合の顧客管理モジュール１４における課金処理の流れについて説明する。

【００５１】当該第２の契約形態のように、伝送された情報量（前記暗号鍵の配信回数や接続時間、データ伝送量）に応じた課金を行う場合には、前述したように図１の鍵管理モジュール１２における暗号鍵の配信回数や、図１のデータモニタシステム１３におけるアドレス毎のデータ量（或いはパケット数）又は接続時間、データ伝送量等の集計情報の取得／集計結果が、顧客認証／鍵管理モジュール制御部２３に転送される。顧客認証／鍵管



理モジュール制御部２３では、この集計情報の取得／集計結果に基づいて、利用履歴ログ収集部２４に対して当該データの提供を受けた契約者（受信側端末２）の利用履歴のログを取り、利用料課金処理部２５に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、請求・収納・支払・滞納管理部２６を介して与信／決済システム５に対して契約者への請求書の発行依頼等を行う。

【００５２】次に、前記第３の契約形態（コンテンツ課金）を行う場合の顧客管理モジュール１４における課金処理の流れについて説明する。

【００５３】当該第３の契約形態のように、受信するデータ種別によって課金がなされる場合は、先ずデータサーバ１０からコンテンツ課金を行うデータ種別の一覧（コンテンツの一覧）がコンテンツ課金設定部２２経由でコンテンツ管理サーバ２０に転送されコンテンツリストに載せられることにより、データ種別の登録が行われる。

【００５４】コンテンツ課金設定部２２では、データ種別すなわちコンテンツ種別とそのコンテンツの暗号化のための暗号鍵の設定を、鍵設定通知として鍵管理モジュール１２に指示する。

【００５５】ここで、一旦、コンテンツ管理サーバ２０にデータ種別が登録されれば、後は第１の契約形態（フラット課金／定額制課金）の場合と同様の処理が行われる。すなわち、特定のデータ種別（特定のコンテンツ）の配信の要求（リクエスト）があった場合、顧客認証／鍵管理モジュール制御部２３は、当該要求者が顧客データベース２１に登録された契約者であるか否かを判断し、またこのリクエストを行った契約者の契約情報をチェックし、暗号鍵を与えて良いか否かを判断し、さらに、与えて良いと判断された場合に、そのリクエストされたデータ種別がコンテンツ管理サーバ２０のコンテンツリストに登録されているかの確認を行い、当該リクエストのあったデータ種別がコンテンツリストに登録されていると確認した場合には、そのリクエストされたデータ種別に対応する鍵配信を鍵管理モジュール１２に指示する。また同時に、顧客認証／鍵管理モジュール制御部２３では、利用履歴ログ収集部２４に対して配信の要求を行った契約者とそのリクエストされたデータ種別の利用履歴の登録を行い、利用料課金処理部２５に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、請求・収納・支払・滞納管理部２６を介して与信／決済システム５に対して契約者への請求書の発行依頼等を行う。

【００５６】次に、本発明実施の形態のデータサービスシステムのより概略的な構成、前記データサーバ１０でのＩＰデータグラムの生成及び暗号化モジュール１１における暗号化処理（セクションデータの生成処理）の詳細及び具体的構成、当該セクションデータ及びそのヘッ

11

ダに含まれるＭＡＣアドレス等の詳細、鍵管理モジュール１２が管理する暗号鍵及びこの暗号鍵の送信並びに暗号化等の詳細、復号化モジュール１５における暗号解読の詳細について、以下に説明する。

【００５７】本発明実施の形態のデータサービスシステムは、図３に示すように、通信経路とされる衛星回線３、専用線３７、電話回線３８、及び双方向の通信経路３９を介して、前記データ送信装置１から前記受信側端末２であるデータ受信装置２ａ，２ｂ，２ｃに対してデータを配信するようになされており、上記データ送信装置１でデータを暗号化し、当該暗号化したデータをデータ受信装置２ａ，２ｂ，２ｃに通信経路を介して伝送するデータサービスシステムである。

【００５８】このデータサービスシステムは、データ送信装置１からデータ受信装置２ａ，２ｂ，２ｃへのデータの伝送に使用する第１の通信経路とされる通信衛星３４を利用した通信経路と、データ送信装置１とデータ受信装置２ａ，２ｂ，２ｃとの間を双方向通信可能にする第２の通信経路である専用線３７、電話回線３８、及び双方向の通信経路３９とを有している。そして、データサービスシステムは、データ送信装置１からデータ受信装置２ａ，２ｂ，２ｃへ送る暗号化したデータの伝送には、上記第１の通信経路を用い、データ送信装置１からデータ受信装置２ａ，２ｂ，２ｃへの前記暗号鍵の伝送には、上記第２の通信経路を用いている。第２の通信経路は、前記インターネット４と接続されている。

【００５９】上記データ送信装置１は、上記各通信回線を利用してデータ受信装置２ａ，２ｂ，２ｃへの各種データの配信を行う。データ受信装置２ａ，２ｂ，２ｃは、各通信回線から伝送されてくるデータを受信する。なお、図１には、データ受信装置２ａ，２ｂ，２ｃを３台として示しているが、実際には数百台から数万台のデータ受信装置（受信側端末２）が存在して当該データサービスシステムを構成している。

【００６０】このデータ送信装置１とデータ受信装置２ａ，２ｂ，２ｃ（なお、以下の説明では、データ受信装置２ａ，２ｂ，２ｃについて特定する必要がない場合には、単にデータ受信装置２という。）との間でデータの送受信を可能にする通信経路については、次のように構成されている。

【００６１】上記衛星回線３は、約３０Ｍｂｐｓの帯域を持ったＫｕバンドの片方向の回線を想定する。この衛星回線３により、例えば、日本全国に分布されているデータ受信装置に対して、データ送信装置１からのデータの伝送を同時期に行うことができる。

【００６２】双方向の通信経路３９は、データ送信装置１とデータ受信装置２との間で、衛星回線３とは別に設けた通信経路であって、データ送信装置１とデータ受信装置２との間でので双方向通信を可能にするものである。本実施の形態では、双方向の通信経路３９は、インターネット４での通信に用いる汎用の通信経路を想定している。

12

【００６３】専用線３７は、データ送信装置１とデータ受信装置２とを直接接続している通信手段である。

【００６４】上記インターネット４は、いわゆる映像情報、音楽情報等の各種情報を提供するものであって、いわゆるインターネットサービスプロバイダ３５により、インターネット４とデータ受信装置２とは通信可能に接続されている。データ送信装置１は、インターネット４に接続されている。

【００６５】なお、上述したようにデータ送信装置１とデータ受信装置２との間でデータの送受信を可能にする専用線３７、電話回線３８、及び双方向の通信経路３９は、衛星回線３ほど大容量の帯域ではなく、数Ｋｂｐｓから数百Ｋｂｐｓ程度が通常の帯域とされる。

【００６６】上記データサービスシステムは、所定のデータを特定のデータ受信装置においてのみ受信することが可能になされており、例えばデータ受信装置２ａのみにデータを伝送するといった個別配信（ユニキャスト型データ配信）、又は例えばデータ受信装置２ａ，２ｂとからなる受信グループにのみデータを伝送するといったグループ宛の同報配信（マルチキャスト型データ配信）、又は全てのデータ受信装置２ａ，２ｂ，２ｃに同時にデータを伝送するといった一斉配信（ブロードキャスト型配信）等の配信形態が可能とされて構成されている。

【００６７】次に、このデータサービスシステムにおいて、データ送信装置１からデータ受信装置２へのデータの伝送について説明する。

【００６８】データ送信装置１からデータ受信装置２へ伝送されるデータは、図４に示すように、データのカプセル化が施されている。このカプセル化は、データを伝送するデータ送信装置１において行われる処理であって、第１のカプセル化工程により、データ受信装置２への配信対象とされるデータを第１のプロトコルによりカプセル化し、第２のカプセル化工程により、上記第１のプロトコルによりカプセル化したデータを第２のプロトコルによってカプセル化する。ここで、カプセル化とは、データ自体に対して加工を施すことなく、当該データ自身を通信プロトコルにより規定された伝送フォーマットに基づいて構成されるカプセル（パケット又はフレーム等）に入れ込むことをいい、このカプセル化によりデータの伝送制御が可能になる。

【００６９】上記第１のカプセル化工程では、データ受信装置２への配信対象とするデータの全体を含む実データ部に当該実データ部に関する付加情報部を付加してカプセル化するとともに、上記実データ部については暗号化して上記カプセル化を行う。以下に詳しく説明する。

【００７０】ＩＰ（Internet Protocol）データグラム１０１は、図４の（ａ）に示すように、インターネット

プロトコルに則して構成されているデータである。このＩＰデータグラム１０１は、上記データ受信装置２への配信対象とされるデータを格納して構成されている。そして、ＩＰデータグラムのヘッダ部には、例えば、インターネット上において使用される宛先を識別するための送信先アドレス（Destination Address）が付加されている。

【００７１】なお、ＩＰデータグラム１０１の部分は、インターネットプロトコルとして構成されることに限定されるものではなく、イーサネットプロトコルを採用して構成されてもよい。

【００７２】そして、データ送信装置１は、図４の（ｂ）から図４の（ｄ）に示すように、データを上記第１のプロトコルによりカプセル化する。例えば、第１のプロトコルとしては、ＤＶＢ（Digital Video Broadcasting）のMultiprotocol Encapsulationを採用している。

【００７３】先ず、データ送信装置１は、第１のプロトコルによるデータのカプセル化を、図４の（ｂ）に示すように、ＩＰデータグラムに対してパディングを行い（パディング部１０２を付加する）、データ部の長さを６４ビットの整数倍にする。例えば、ＩＰデータグラム１０１の末尾に０ビット～６３ビット長のパディングを行い、パディングするビットはすべて１とする。このパディングにより、所定のデータ長さにすることができ、これは、このＩＰデータグラム１０１とパディング部１０２とからなるセクションのデータ部を暗号化する際に、データ部の長さが６４ビットの整数倍の方が都合が良いからである。本実施の形態では、当該第１のプロトコルのフォーマットによって構成されるデータ部分をセクションと呼んでいる。

【００７４】次に、データ送信装置１は、パディング部１０２が付加されたセクションを、図４の（ｃ）に示すように暗号化する。ここで、暗号化は、暗号鍵によって行うもので、暗号鍵は、上記データ受信装置２に対して配信の対象とされる情報について暗号化するために使用される後述するセッション鍵である。また、暗号化の方式としては、いわゆるTriple-DESのような共通鍵方式のブロック暗号化を用いる。このTriple-DES方式の暗号化は、公開鍵方式の中でも強力な暗号方式であり、ハードウェアによる実装で高速化も容易とされる。これにより、３０Ｍｂｐｓ程度の高速な暗号化にあっても、公開鍵方式の暗号化とは異なり、処理時間がかかってデータの伝送が間に合わなくなることを防止することができる。

【００７５】そして、データ送信装置１は、図４の（ｄ）に示すように、暗号化されたセクションデータ部１０４に、セクションヘッダ部１０３及びエラー検出のために使用されるテイラ部１０５を付加する。

【００７６】ここで、上記暗号化されたセクションデータ部１０４は、ＭＡＣ（Media Access Control）フレーム化されて構成されている。このＭＡＣフレーム化により、データ部にＭＡＣヘッダが付加され、このＭＡＣヘッダ部を参照することにより、当該フレーム化されて格納されているデータの宛先の制御が容易となされるようになる。具体的には、ＭＡＣフレームには、当該ＭＡＣフレーム化されたデータの受信が許可されているデータ受信装置の宛先アドレスが格納されている。

【００７７】上記セクションヘッダ部１０３は、宛先アドレスを格納する部分であって、４８ビットの宛先アドレスが格納されるようにデータ空間が確保されている。具体的には、上記セクションヘッダ部１０３においてＭＡＣヘッダ部を構成して、宛先アドレスが格納されている。このセクションヘッダ部１０３に４８ビットにより表現される宛先アドレスを格納できる空間を設けることにより、データ受信装置の限定範囲の種類が少ないことを解消することができる。すなわち、暗号鍵を識別するための多くの情報を格納することができるようになる。さらに、ＩＰデータグラム１０１を伝送する際に、インターネットプロトコルの宛先アドレスから後述するパケットＩＤの対応付けを行わなくもよくなり、インターネットプロトコルとの親和性を得ることができる。

【００７８】また、上記テイラ部１０５は、ＣＲＣ（Cyclic Redundancy Checking、巡回冗長検査）によってコード化されている。ＣＲＣは、ＭＡＣフレーム化されたデータを受信したデータ受信装置２が、当該ＭＡＣフレームが正しく衛星回線において伝送されているかを検査するためのものである。例えば、ＣＲＣは、３２ビットによってコード化されている。

【００７９】以上が第１のプロトコルによる配信対象とされるデータのカプセル化であって、次に、この第１のプロトコルによってカプセル化されたデータを、第２のプロトコルによってカプセル化させる処理について説明する。

【００８０】第２のプロトコルによるカプセル化は、上記第１のプロトコルによってカプセル化されたデータを、複数のパケットに分割することにより実行されるカプセル化である。

【００８１】ここで、第２のプロトコルは、ＴＳ（Transport Stream）パケット化によるものである。ＭＰＥＧ２（Moving Picture Experts Group Phase 2）によって規格されているものであって、オーディオ、ビデオ信号やデータのような多種類のデータが多重化されて、大容量のディジタル回線で伝送することが可能になる。この第２のプロトコルにより、上記第１のプロトコルによってカプセル化されたデータは、図４の（ｅ）乃至図４の（ｇ）に示すように、カプセル化されて、複数のＴＳパケット１０６，１０７，１０８に分割される。上記ＴＳパケット１０６，１０７，１０８は、ＴＳヘッダ部HTSと、ＴＳペーロード部Ｐとによって構成され、上記ＴＳ

15

ペイロード部Ｐには、分割されて上記第１のプロトコルによってカプセル化されたデータが格納される。そして、ＴＳパケットのＴＳヘッダ部HTSには、図５に示すような、パケットＩＤ（ＰＩＤ）部及びスクランブル制御部によって構成される。この図５は、一般的なＴＳパケットのフォーマットの構造を表しており、ヘッダ部のＰＩＤ (Packet Identification) 部４１１及びスクランブル制御部４１２により暗号鍵が特定される。当該暗号鍵は、セッション鍵Ｋｓとワーク鍵Ｋｍとがある。また、上記ＰＩＤ部４１１は１３ビットのデータであり、上記スクランブル制御部４１２は２ビットのデータ、ＴＳパケットのデータはペイロード部分４１３に記述される。なお、この図５の例では、ＰＩＤ部４１１及びスクランブル制御部４１２に宛先アドレスが書き込まれているが、本実施の形態においては、上述したように、宛先アドレスをセクションヘッダ部１０３に書き込むことにより、宛先アドレス情報が制限されることを防止している。

【００８２】以上が第２のプロトコルによるカプセル化であり、よって、データ送信装置１は、データ受信装置２への配信対象とされるデータ（ＩＰデータグラム）を第１のプロトコル及び第２のプロトコルによって多重にカプセル化して、通信衛星３４への当該データの伝送を行っている。

【００８３】このように、本実施の形態では、ＴＳパケットとセクションの２つのレベルにおいてそれぞれ独立に処理してデータ伝送を行っているので、例えば利用するＰＩＤを増加することなく、暗号鍵について多くの情報を確保することができ、また、アプリケーション毎に制御方法を用意しなくて済み、新しいアプリケーションへの素早い対応がでいるようになり、さらに、認証ヘッダや暗号ペイロードを既存のインターネットで使うことができるようになる。

【００８４】次に、データ送信装置１において行う暗号鍵によるデータの暗号化及びデータ受信装置２において行う暗号化されているデータの暗号鍵（復号鍵）による復号化について説明する。

【００８５】ここで、データ送信装置１における前記鍵管理モジュール１２及び暗号化モジュール１１と、データ受信装置２の前記鍵受信モジュール１６及び復号化モジュール１５は、具体的には図６に示すように構成されている。

【００８６】この図６において、セッション鍵Ｋｓ１２４及び１３４は、上記データ送信装置１及び上記データ受信装置２がデータの暗号化／復号化に使用する鍵であり、いわゆる共通鍵方式が採用されている。上記データ送信装置１のセッション鍵Ｋｓ１２４は前記鍵管理モジュール１２が管理し、上記データ受信装置２のセッション鍵Ｋｓ１３４は鍵受信モジュール１６が復号化して生成する。

16

【００８７】データ送信装置１の暗号化ユニット１２１は、セッション鍵Ｋｓ１２４を使用して、特定のデータ受信装置に対して送られる情報データを暗号化する。すなわち図１の暗号化モジュール１１は、図４の（ｃ）に示すセクションのデータ部を、当該セッション鍵Ｋｓ１２４を使用して上記Triple-DESにより暗号化する。また、データ受信装置２の復号化ユニット１３１は、配信されてきた暗号化されたデータをセッション鍵Ｋｓ１３４により復号化して意味のある情報として取り出す。

【００８８】マスター鍵Ｋｍ１２５及びＫｍ１３５は、上記セッション鍵Ｋｓと同様に、データ送信装置１及びデータ受信装置２が共に所持している暗号鍵であって、各データ受信装置２ａ，２ｂ，２ｃに固有のものである。

【００８９】マスター鍵Ｋｍは、データ送信装置１とデータ受信装置２と間を送信処理されるようなことはなく、すなわち、通信経路上に存在する場合はなく、これによりいかなる手段によっても他人によって知ることができない暗号鍵とされている。

【００９０】このマスター鍵Ｋｍは、セッション鍵Ｋｓをデータ送信装置１からデータ受信装置２に送信する際に、セッション鍵Ｋｓを暗号化／復号化するために用いられる。すなわち、データ送信装置１の鍵管理モジュール１２に内蔵される暗号化ユニット１２２は、マスター鍵Ｋｍ１２５を使用してセッション鍵Ｋｓ１２４を暗号化してデータ受信装置２に予め伝送しておく。データ受信装置２の鍵受信モジュール１６に内蔵される復号化ユニット１３２は、受信した暗号化されているセッション鍵Ｋｓ１２４を、当該データ受信装置２が所持しているマスター鍵Ｋｍ１３５によって復号化して取り出す（セッション鍵Ｋｓ１３４として取り出す）。

【００９１】このマスター鍵Ｋｍによる暗号鍵（セッション鍵Ｋｓ）の暗号化及び復号化により、データ送信装置１からデータ受信装置２へ伝送する間に、上記暗号化されたセッション鍵Ｋｓが盗聴者によって盗聴されたとしても、その復号化がなされることはない。

【００９２】なお、このマスター鍵Ｋｍによるセッション鍵Ｋｓの暗号化／復号化についても、上記Triple-DESに基づいて行うが、公開暗号方式を採用することもできる。これは、公開暗号方式は、鍵の暗号化及び復号化がデータの暗号化／復号化とは異なり高速性を要求されないこと、安全性を確保することができるからである。

【００９３】本実施の形態では、上記セッション鍵Ｋｓ１２４を、前述したように顧客管理モジュール１４の管理の元で鍵管理モジュール１２が管理し、このセッション鍵Ｋｓ１２４の配信状況に応じて前述したような課金が行われる。

【００９４】ここまでの説明では、データ受信装置２がデータ送信装置１から受動的にセッション鍵Ｋｓ１２４を受け取る例を説明したが、双方向通信経路９を利用す

ることにより、データ受信装置２の側から能動的にセッション鍵Ｋｓの要求を行うこともできる。これにより、各データ受信装置２ａ，２ｂ，２ｃは、素早く確実に必要なセッション鍵Ｋｓ１２４をデータ送信装置１から取得することができる。具体的には、例えば、新たにデータ受信装置２がこのデータサービスシステムに加わる場合や、障害によりこの系から外れていたデータ受信装置２が障害から復旧して再びこのデータサービスシステムに加わる場合、またデータ受信装置２においてセッション鍵Ｋｓが正しく受信出来なかった場合などには、データ受信装置２の側から能動的にセッション鍵Ｋｓの要求を行うことにより、各データ受信装置２ａ，２ｂ，２ｃは素早く確実に必要なセッション鍵Ｋｓを取得することができる。例えば、上述したような障害復旧やセッション鍵Ｋｓの更新の管理は、データ送信装置１の鍵管理モジュール１２や、データ受信装置（受信側端末）２内にある鍵受信モジュール１６及びデータ表示リクエストモジュール１７等が、双方向に通信を行うことにより実現する。このようなことから、本実施の形態においては、例えば衛星回線のみをデータサービスシステムに組み込むことによる弊害、例えば、情報が各データ受信装置に正しく伝わったかどうかをデータ送信装置が知ることができない等といった問題を解決することができる。

【００９５】なお、データ送信装置１からデータ受信装置２へのセッション鍵Ｋｓの伝送については、片方向通信経路とされる衛星回線３を用いて行ってもよく、双方向の通信経路３９によって行ってもよい。

【００９６】ここで、上記セッション鍵Ｋｓは、前記第３の暗号鍵変更タイミングのように、定期的に更新して配信される場合がある。このセッション鍵Ｋｓの更新は、図７に示すフローチャートのような更新手順に従って実行される。

【００９７】先ず、ある時点において、データ受信装置２の鍵受信モジュール１６は、セッション鍵Ｋｓ１３４として、セッション鍵Ks_evenと、セッション鍵Ks_oddの２つを保持している。データ受信装置２は、このようにセッション鍵Ｋｓを２つ所持することにより、このセッション鍵Ks_even又はセッション鍵Ks_oddの何れかを使用して、データ送信装置１から送信されてくる情報データの復号化を行う。

【００９８】ここで、現在使っているセッション鍵Ｋｓがどちらであるかは、前記図４に示すセッションヘッダ部１０３に情報として書き込まれている。例えば、セクションヘッダ部１０３は、図８に示すように、テーブルＩＤ（table_id）、ＭＡＣアドレス部（MAC_address_1, MAC_address_2, MAC_address_3, MAC_address_4, MAC_address_5, MAC_address_6）と、セクション情報部（section_length, section_number, last_section_number）、ｓｓｉ（section_syntax_indicator）、ｐｉ（private_indicator）、ｒｓｖｄ（reserved）、ｐｓｃ（payload_scramble_indicator）１１１、ａｓｃ（address_scramble_indicator）、ＬＳｆ（LLC_SNAP_flag）、及びｃｎｉ（current_next_indicator）によって構成さている。ここで、ｐｓｃ１１１が現在使っているセッション鍵Ｋｓがどちらであるかの情報を示す。例えば、上記ｐｓｃ１１１は、２ビットの情報であり、例えば、ｐｓｃの上位ビットが「０」のときは、セッション鍵Ks_evenが使用されていることを示し、ｐｓｃの上位ビットが「１」のときには、セッション鍵Ks_oddが使用されていることを示す。



【００９９】上述したような使用されているセッション鍵Ｋｓの判断をステップＳ１において行った後、データ受信装置２の鍵受信モジュール１６は、ステップＳ２において、タイマーでトリガをかけ、セッション鍵Ｋｓの更新タイミングを知る。

【０１００】続いて、データ受信装置２の鍵受信モジュール１６は、ステップＳ３において、ＭＡＣアドレスとセッション鍵Ｋｓの対応表にある現在のセッション鍵Ｋｓのフラグを更新する。データ受信装置の鍵受信モジュール１６は、例えば、図９のＭＡＣアドレスとセッション鍵Ｋｓの対応表を有しており、この対応表を参照して、現在のセッション鍵Ｋｓのフラグ１１２を更新する。この更新処理により、上記のｐｓｃ１１１の上位１ビットが反転する。例えば、ｐｓｃの上位ビットが「０」に反転される。

【０１０１】そして、データ受信装置２では、ステップＳ４において、そのｐｓｃに基づいてそのセクションに含まれているＩＰデータグラムの復号化を行う。すなわち、ｐｓｃの上位ビットが「０」とされた場合には、データ受信装置２の鍵受信モジュール１６は、これまで使用していたセッション鍵Ks_odd（ｐｓｃの上位ビットが「１」のとき使用されるセッション鍵Ｋｓ）からセッション鍵Ks_evenに変更し、復号化モジュール１５ではこのセッション鍵Ks_evenにより復号化を行う。また、ｐｓｃの上位ビットが「１」とされた場合には、データ受信装置２の鍵受信モジュール１６は、これまで使用していたセッション鍵Ks_even（ｐｓｃの上位ビットが「０」のとき使用されるセッション鍵Ｋｓ）からセッション鍵Ks_oddに変更し、復号化モジュール１５ではこのセッション鍵Ks_oddにより復号化を行う。

【０１０２】そして、次のセッション鍵Ｋｓの切替えのタイミングまでの間に、ステップＳ５において、データ送信装置１の鍵管理モジュール１２では、次のセッション鍵Ｋｓをマスター鍵Ｋｍ１２４により暗号化してデータ受信装置２に転送する。

【０１０３】なお、暗号化されたセッション鍵Ｋｍ（Ｋｓ）の転送は、衛星回線３又は双方向の通信回線３９を使って伝送するが、その伝送の際のプロトコルについては、応答の伴うプロトコルを用い、例えばＴＣＰ／ＩＰ（Transmissiom Control Protcol／Internet Protoco

l）を使用する。これにより、データ送信装置１からデータ受信装置２へのセッション鍵Ｋｓの伝送が確実に行われる。

【０１０４】そして、この転送処理の間に、ステップＳ６において、データ受信装置２の鍵受信モジュール１６は、図９に示すＭＡＣアドレスのセッション鍵Ｋｓの対照表の更新を行う。すなわち、以前使用していたセッション鍵Ｋｓを、新しいセッション鍵Ｋｓに書き換える処理を行う。

【０１０５】その後、ステップＳ７において、データ受信装置２の鍵受信モジュール１６は、対象とするデータ受信装置２に次のセッション鍵Ｋｓが保持されたかを確認した後に、ステップＳ８に進み、次のセッション鍵Ｋｓに切り替える。ここで、ステップＳ８以降ステップＳ１３までの処理は、ｐｓｃの上位ビットが「１」とされて、セッション鍵Ks_oddを復号化に使用するときの処理であって、上記ステップＳ７から進む処理であり、また、上記ステップＳ１において、データ受信装置２にて現在のセッション鍵Ｋｓがセッション鍵Ks__even（ｐｓｃの上位ビットが「０」）とされたときに実行される処理でもある。

【０１０６】上述したような手順により、データ送信装置１は、更新されるセッション鍵Ｋｓを確実にデータ受信装置２に届けることができ、データ受信装置２では、２つ所持するセッション鍵Ｋｓを切替えを瞬時に行い、データの取りこぼしもなくセッション鍵Ｋｓによる復号化を実現することができる。なお、伝送処理時間の許す範囲で、セッション鍵Ｋｓ１２４の更新頻度は柔軟に変更することが可能である。

【０１０７】以上のようにセッション鍵Ｋｓがデータ送信装置１において逐次変更されている場合でも、データ受信装置２は、このように変更されるセッション鍵Ｋｓによって暗号化されているデータの復号が可能である。

【０１０８】次に、データ送信装置１がデータを送信するまでの手順、及びデータ受信装置２がデータを受信したときの手順について説明する。データ送信装置１がデータを送信するまでの手順については、例えば、図１０に示すフローチャートに従って実行している。そして、データ受信装置２がデータを受信してからの手順については、例えば、図１１に示すフローチャートに従って実行している。

【０１０９】先ず、データ送信装置１がデータを送信するまでの手順については、ステップＳ２１において、データ送信装置１は、データ受信装置２に伝送するＩＰデータグラムを、データ送信装置１自身又は双方向の通信経路３９に繋がるインターフェースより、受け取る。また、インターネット４上からのアクセス情報に基づいて、情報センタの情報の提供を受け取る。

【０１１０】次にステップＳ２２において、データ送信装置１は、ＩＰデータグラムの宛先アドレスを見て、第



１のプロトコルの宛先アドレスを知る。例えば、データ送信装置１は、当該データ送信装置１内に所持している図１２に示すようなＩＰアドレスとＭＡＣアドレスの対応表からデータ受信装置２の第１のプロトコルでの宛先アドレスを知る。

【０１１１】そして、宛先アドレスを知ったデータ送信装置１は、その宛先アドレスをもとに上記セクションを作成する。ここで、データ送信装置１は、必要に応じてデータ部にビット１によるパディングを行い、データ部が６４ビットの倍数になるようにする。

【０１１２】次に、ステップＳ２３において、例えば図９に示したようなＭＡＣアドレスとセッション鍵Ｋｓの対応表から現在のセッション鍵Ｋｓのフラグ１１２を見て、現在使用しているセッション鍵Ｋｓ１２４を取り出し、当該取り出したセッション鍵Ｋｓにより、上記図４の（ｃ）に示すように、セクションのデータ部を暗号化する。その際、現在のセッション鍵Ｋｓのフラグを見て、その内容を上記図９に示すセッションのヘッダ部のｐｓｃ１１１の上位１ビットに入れる。

【０１１３】次にステップＳ２４において、図４の（ｅ）乃至図４の（ｇ）に示すように、このセクション全体１０９を分割して各ＴＳパケット１０６，１０７，１０８のペイロード部Ｐに入れ、当該ＴＳパケット１０６，１０７，１０８に予め定められた上記ＰＩＤを付加し、さらに、第２のプロトコルの必要に応じてペイロード部Ｐを暗号化し、衛星回線３に送出する。

【０１１４】以上がデータ送信装置２がデータを送信するまでの手順である。そして、データ受信装置２では、上述のようにして衛星回線３に送出されたデータを受信する。

【０１１５】データ受信装置２は、先ず図１１のステップＳ３１において、 衛星回線３より受信したＴＳパケット１０６，１０７，１０８を第２のプロトコルに従って復号化し、セクション全体１０９を再構築する。

【０１１６】次に、ステップＳ３２において、データ受信装置２は、セクションの宛先アドレス（ＭＡＣアドレス）を取り出し、続いて、ステップＳ３３において、図１３に示すＭＡＣアドレスとセッション鍵Ｋｓの対応表を参照してＭＡＣアドレスが存在するか否かの判別処理を行う。すなわち、自己に送信が許可されているデータを格納しているものであるか否かの判別処理を行う。ここで、ＭＡＣアドレスがないことを確認した場合には、データ受信装置２は、ステップＳ３４に進み、そのデータの破棄の処理を行う。また、ＭＡＣアドレスがあることを確認した場合には、データ送信装置２は、ステップＳ３５に進み、セクションヘッダ部１０３より前記図８に示したｐｓｃ１１１を取り出す。そして、データ送信装置２は、そのｐｓｃ１１１の上位１ビットから現在有効なセッション鍵Ｋｓがどちらであるかを調べ、２つのセッション鍵Ｋｓから現在有効とされるセッション鍵Ｋ

ｓを取り出す。

【０１１７】データ受信装置２は、このようにして取り出したセッション鍵Ｋｓにより、ステップＳ３６において、セクションデータ部１０４をTriple-DESにより復号化する。

【０１１８】そして、データ受信装置２は、ステップＳ３７において、当該復号したデータからＩＰデータグラムを取り出す。例えば、ＩＰデータグラムの取り出しは、復号化されたデータ部の先頭にあるＩＰヘッダから図１４のTOTAL LENGTH フィールド１１３を読み取り、ＩＰデータグラムの長さを調べ、そこから計算されるＩＰデータグラム全体を取り出す。これにより、暗号化の際に付加した余計なパディングを除去される。このようにして目的とするＩＰデータグラムを取り出すことができる。

【０１１９】以上のような手順により、データ送信装置１は、データを送信するまでの処理を行い、また、データ受信装置２は、受信したデータに対する処理を行い、自己に宛てて配信されてきた情報データを受け取る。

【０１２０】なお、本実施の形態のデータサービスシステムは、次のように変形することも可能である。

【０１２１】すなわち、第１の変形例として、データサービスシステムは、図１５に示すように構成することも可能である。この図１５に示すデータサービスシステムは、データ受信装置２がＩＰルータとして構成される場合である。

【０１２２】ところで、上述したデータサービスシステムでは、データ受信装置２が直接ＩＰデータグラムを受信する構成としている。しかし、このデータサービスシステムでは、データ受信装置２をＩＰルータとして構成することにより、データ受信装置２が衛星回線３から受信したデータを、イーサネットなどのローカルエリアネットワーク（ＬＡＮ）２０２を経由してつながっている衛星回線３へのインターフェースを持たないコンピュータ２０３ａ，２０３ｂにもデータを伝送することができる。その際、データ送信装置１やデータ受信装置２は、データ受信装置２だけでなく、それがつながっているローカルエリアネットワーク２０２上のコンピュータ２０３ａ，２０３ｂ全てについてのデータの配信を行うことができるようになる。具体的には、図１２に示したデータ送信装置１内のＩＰアドレスとセクションの宛先アドレス（ＭＡＣアドレス）の対応表のＩＰアドレスが、個別のＩＰアドレスではなく、複数のＩＰアドレスの集合を示すＩＰのネットワークアドレスに変わることになる。但し、このデータサービスシステムにおいて、データ伝送を行うのは衛星回線３の区間のみであるため、データ受信装置２とコンピュータ２０３ａ，２０３ｂとの間でもデータ配信を行うには、ＩＰプロトコル又はそれより上位のアプリケーションのレベルでのデータ配信制御が必要となる。



【０１２３】次に、第２の変形例として、データサービスシステムは、図１６に示すように構成することも可能である。このデータサービスシステムでは、データ受信装置２がブリッジとして構成され、ＩＰデータグラムを伝送するプロトコルの変換のみを行い、上記データ伝送システム２０１とでは、ルーティングを行わないことで異なる。

【０１２４】この場合の上記データ受信装置２は、衛星回線３より受信したデータを復号化してＩＰデータグラムを取り出し、それをイーサネットフレームに入れて汎用のルータ３０２に転送する。そして、汎用のルータ３０２が、通常のＩＰデータグラムに対する処理を行う。これにより、ルーティングを行わないためにデータ受信装置２の構成が簡単になり、既存の汎用のルータを用いることができるようになる。

【０１２５】

【発明の効果】以上の説明で明らかなように、本発明においては、データを暗号化して提供し、暗号化されたデータの当該暗号化を解くための暗号鍵を管理し、暗号鍵を配信し、暗号鍵の配信形態に応じて課金を管理することにより、例えば衛星放送やディジタルＣＡＴＶ回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合において、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現可能としている。

【０１２６】すなわち本発明のデータ伝送システムの課金方法及び装置は、例えば衛星放送や双方向或いは一方向のディジタルＣＡＴＶ回線等の大容量且つ高速のデータ伝送路と、電話回線やＩＳＤＮ等に代表される比較的低速度の回線とを組み合わせることにより、高速のインターネットアクセス等のデータサービスを実現すると共に、ＩＰパケットベースの暗号化における鍵配信の仕組みとデータ提供に対する課金とを組み合わせることにより、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現可能としている。

【図面の簡単な説明】

【図１】本発明のデータ伝送システムの課金方法及び装置が適用されるデータサービスシステムの主要部の構成を示すブロック図である。

【図２】本実施の形態のデータサービスシステムの顧客管理モジュールの構成例を示すブロック図である。

【図３】本発明の実施の形態であるデータサービスシステムの概略的な構成を示す図である。

【図４】本実施の形態のデータサービスシステムを構成するデータ送信装置からデータ受信装置へ送信されるデータであって、複数のプロトコルによってカプセル化が施されたデータを示す図である。

【図５】ＴＳパケットのデータ構造のフォーマットを示す図である。

23

【図６】データ送信装置及びデータ受信装置の構成を示すブロック図である。

【図７】データ送信装置からデータ受信装置へ送信されるデータを暗号化するセッション鍵の変更を行う手続きの一連の工程を示すフローチャートである。

【図８】セクションヘッダのデータ構造を示す図である。

【図９】ＭＡＣアドレスとセッション鍵のフラグとの対応表を示す図である。

【図１０】データ送信装置において行うデータのカプセル化の一連の手続きを示すフローチャートである。

【図１１】データ受信装置が受信したデータをセッション鍵により復号化するときの一連の手続きを示すフローチャートである。

【図１２】ＩＰアドレスとＭＡＣアドレスとの対応表を示す図である。

【図１３】ＭＡＣアドレスとセッション鍵の対応表を示す図である。

【図１４】ＩＰデータグラムの取り出しの際に使用されるTOTALLENGTHフィールドが格納されるデータ構造を示す図である。

24

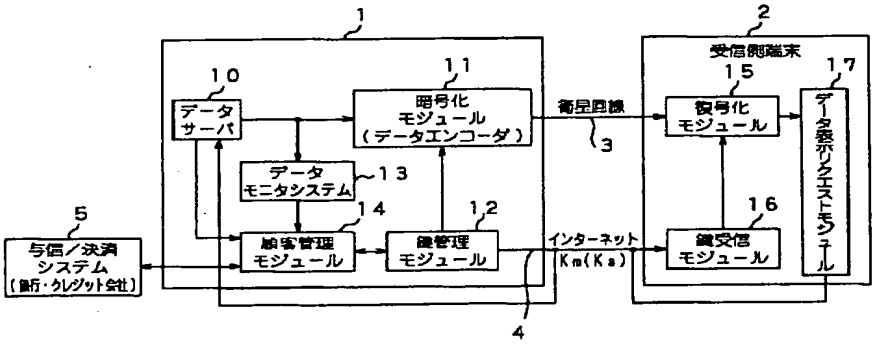
【図１５】本実施の形態のデータサービスシステムの第１の変形例を示す図である。

【図１６】本実施の形態のデータサービスシステムの第２の変形例を示す図である。

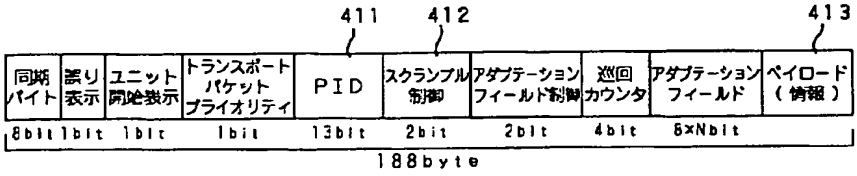
【符号の説明】

１　データ伝送装置、　２　受信側端末（データ受信装置）、　３　衛星回線、　４　インターネット、　５　与信／決済システム、　１０　データサーバ、１１　暗号化モジュール（データエンコーダ）、　１２　鍵管理モジュール、１３　データモニタモジュール、　１４　顧客管理モジュール、　１５　復号化モジュール、　１６　鍵受信モジュール、　１７　データ表示リクエストモジュール、　２０　コンテンツ管理サーバ、　２１　顧客データベース、　２２コンテンツ課金設定部、　２３　顧客認証／鍵管理モジュール制御部、　２４利用履歴ログ収集部、　２５　利用料課金処理部、　２６　請求・収納・支払・滞納管理部、　Ｋｓ　セッション鍵、　Ｋｍ　マスター鍵

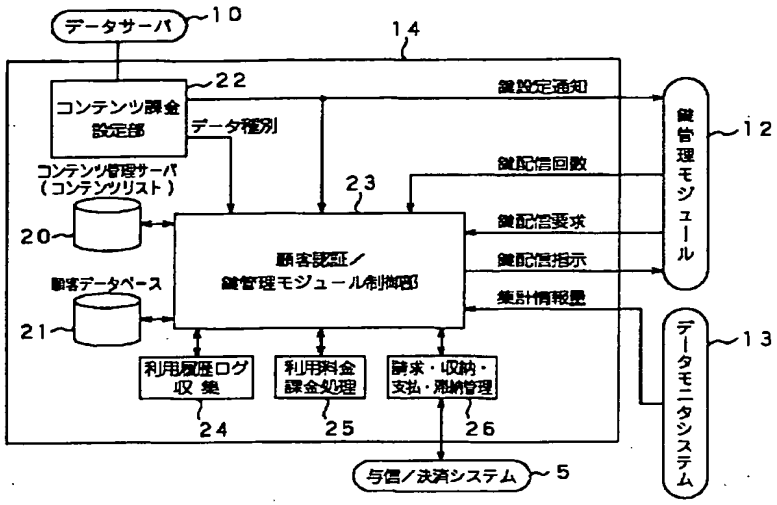
【図１】



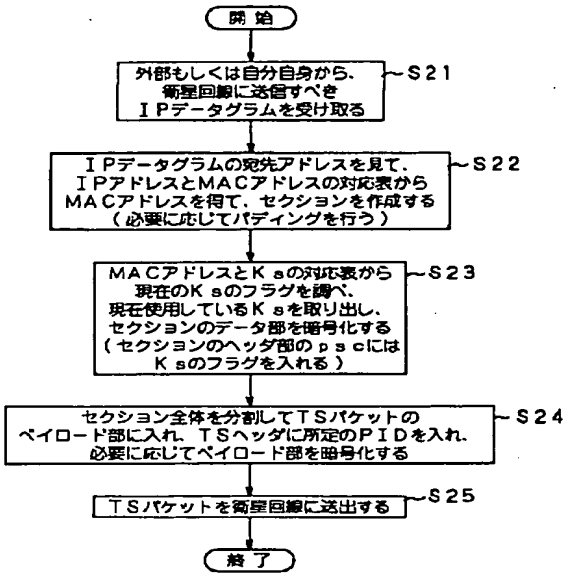

【図５】



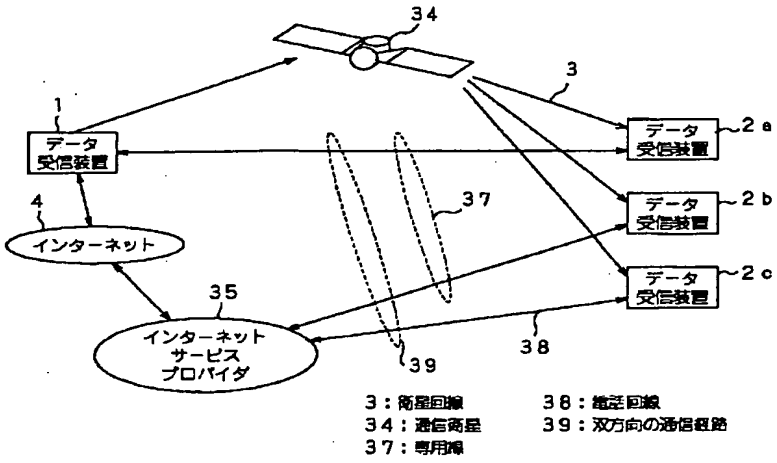
【図２】


データサーバ
10
14
22
コンテンツ課金設定部
データ種別
鍵設定通知
鍵配信回数
鍵配信要求
鍵配信指示
集計情報要
鍵管理モジュール
12
コンテンツ管理サーバ（コンテンツリスト）
20
23
顧客データベース
21
顧客認証／鍵管理モジュール制御部
データモニタシステム
13
利用履歴ログ収集
利用料金課金処理
請求・収納・支払・滞納管理
24
25
26
与信／決済システム
5

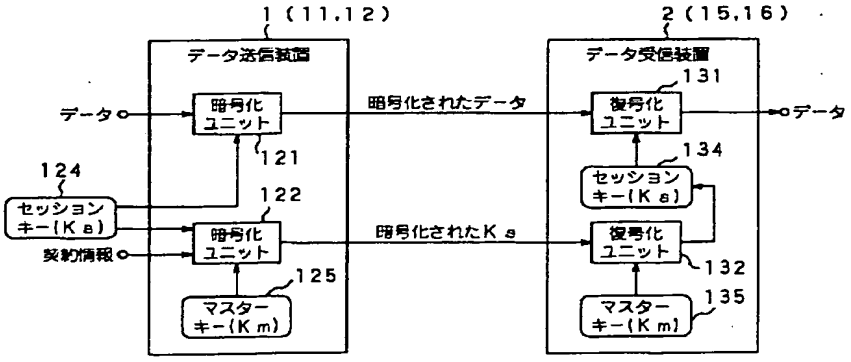
【図１０】


開始
外部もしくは自分自身から、衛星回線に送信すべきＩＰデータグラムを受け取る
S21
ＩＰデータグラムの宛先アドレスを見て、ＩＰアドレスとＭＡＣアドレスの対応表からＭＡＣアドレスを得て、セクションを作成する（必要に応じてパディングを行う）
S22
ＭＡＣアドレスとＫｓの対応表から現在のＫｓのフラグを調べ、現在使用しているＫｓを取り出し、セクションのデータ部を暗号化する（セクションのヘッダ部のｐｓｃにはＫｓのフラグを入れる）
S23
セクション全体を分割してＴＳパケットのペイロード部に入れ、ＴＳヘッダに所定のＰＩＤを入れ、必要に応じてペイロード部を暗号化する
S24
ＴＳパケットを衛星回線に送出する
S25
終了

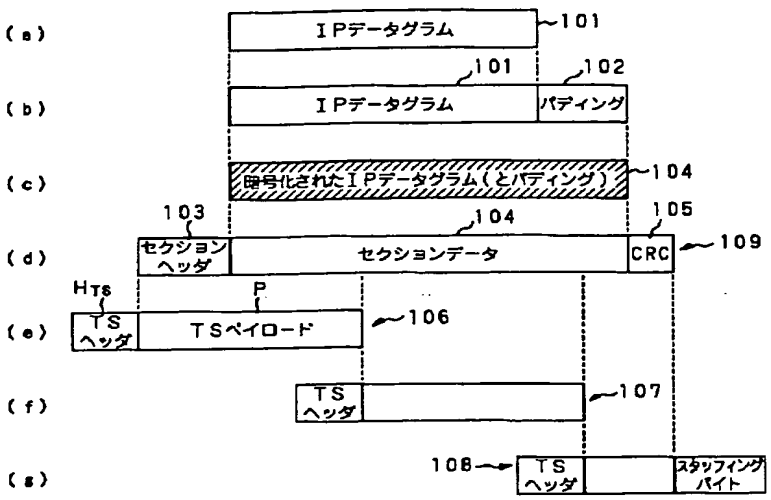
【図３】


34
3
1
データ受信装置
2a
2b
2c
4
インターネット
37
35
インターネットサービスプロバイダ
39
38
3：衛星回線
34：通信衛星
37：専用線
38：地上回線
39：双方向の通信経路

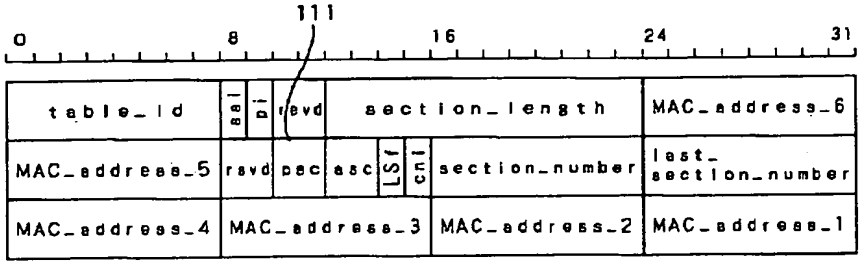
【図６】


1（11,12）
データ送信装置
2（15,16）
データ受信装置
データ
暗号化ユニット
121
暗号化されたデータ
131
復号化ユニット
データ
124
セッション鍵（Ｋｓ）
122
暗号化ユニット
契約情報
暗号化されたＫｓ
134
セッション鍵（Ｋｓ）
復号化ユニット
132
125
マスター鍵（Ｋｍ）
135
マスター鍵（Ｋｍ）

【図４】




【図８】




ssi: section_syntax_indicator
pi: private_indicator
rsvd: reserved
psc: payload_scramble_indicator
asc: address_scramble_indicator
LSf: LLC_SNAP_flag
cni: current_next_indicator

【図９】

| MACアドレス | Ks_even | Ks_odd | Ksフラグ |
|---|---|---|---|
| 08:00:46:01:07:24 | 0xC08F...25 | 0x9083...AF | 0 |
| 08:00:46:01:07:09 | 0x26D2...61 | 0xBA02...3C | 1 |
| 01:00:5e:16:0:0 | 0x461E...67 | 0xDC1A...22 | 0 |

112

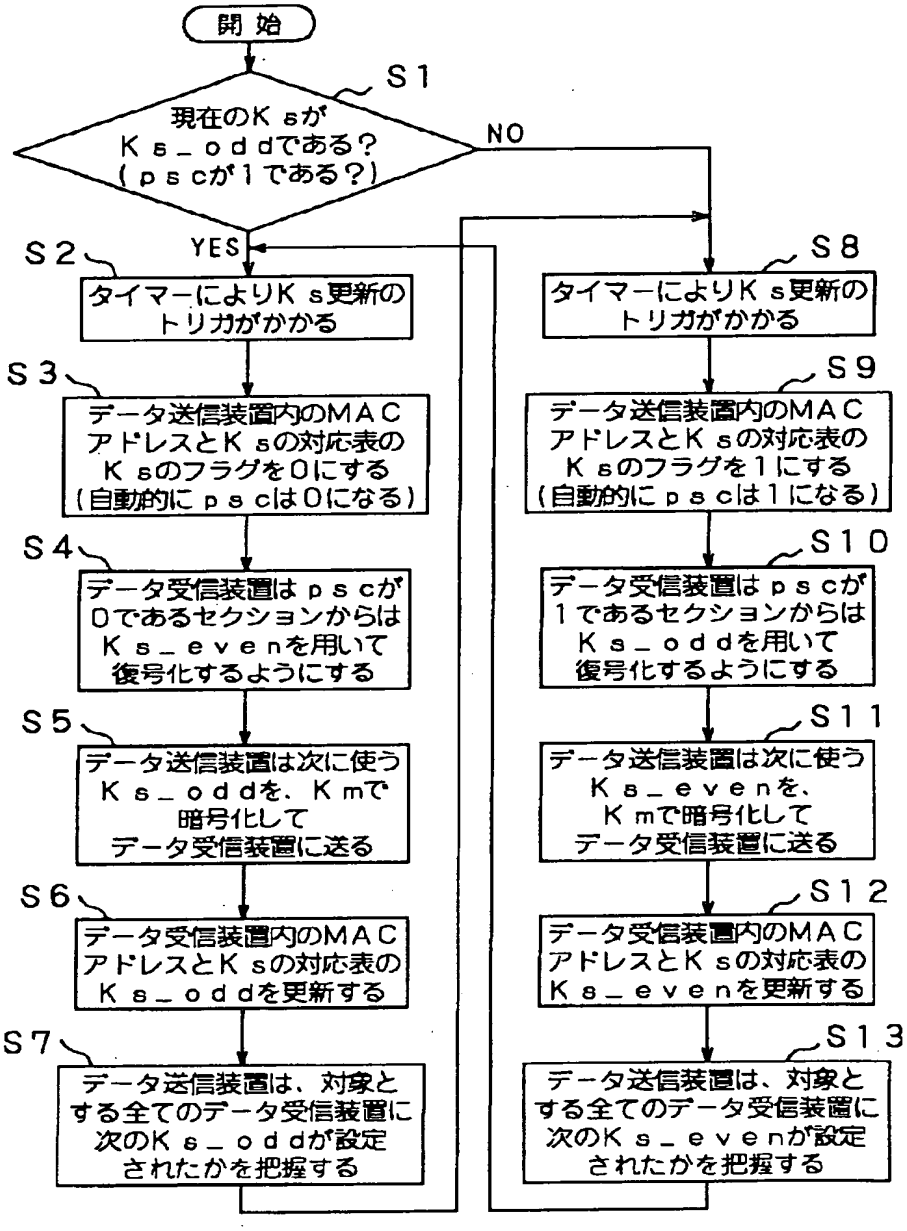
【図１２】

| IPアドレス | bitmask | MAC address |
|---|---|---|
| 133. 11. 9. 39 | 255. 255. 255. 225 | 08:00:46:01:07:24 |
| 133. 11. 20. 0 | 255. 255. 255. 0 | 08:00:46:01:07:09 |
| 226. 0. 0. 0 | 255. 255. 255. 224 | 01:00:5e:16:0:0 |

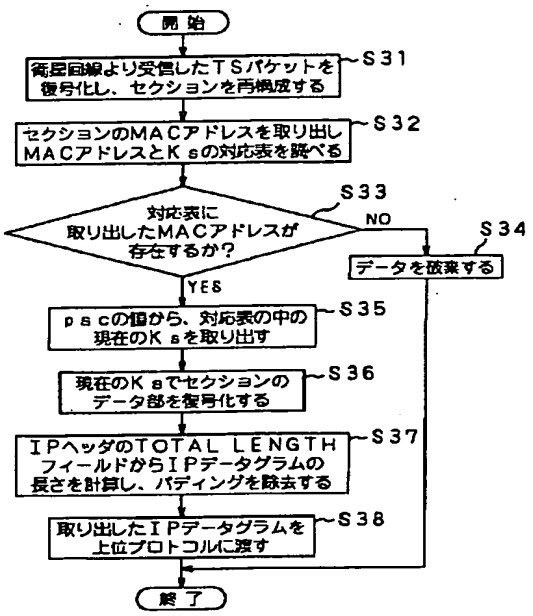
【図１３】

| MACアドレス | Ks_even | Ks_odd |
|---|---|---|
| 08:00:46:01:07:24 | 0xC08F...25 | 0x9083...AF |
| 01:00:5e:16:0:0 | 0x461E...67 | 0xDC1A...22 |

【図７】


開始
S1
現在のＫｓが
Ｋｓ＿ｏｄｄである？
（ｐｓｃが１である？）
NO
YES
S2
タイマーによりＫｓ更新の
トリガがかかる
S3
データ送信装置内のＭＡＣ
アドレスとＫｓの対応表の
Ｋｓのフラグを０にする
（自動的にｐｓｃは０になる）
S4
データ受信装置はｐｓｃが
０であるセクションからは
Ｋｓ＿ｅｖｅｎを用いて
復号化するようにする
S5
データ送信装置は次に使う
Ｋｓ＿ｏｄｄを、Ｋｍで
暗号化して
データ受信装置に送る
S6
データ受信装置内のＭＡＣ
アドレスとＫｓの対応表の
Ｋｓ＿ｏｄｄを更新する
S7
データ送信装置は、対象と
する全てのデータ受信装置に
次のＫｓ＿ｏｄｄが設定
されたかを把握する
S8
タイマーによりＫｓ更新の
トリガがかかる
S9
データ送信装置内のＭＡＣ
アドレスとＫｓの対応表の
Ｋｓのフラグを１にする
（自動的にｐｓｃは１になる）
S10
データ受信装置はｐｓｃが
１であるセクションからは
Ｋｓ＿ｏｄｄを用いて
復号化するようにする
S11
データ送信装置は次に使う
Ｋｓ＿ｅｖｅｎを、
Ｋｍで暗号化して
データ受信装置に送る
S12
データ受信装置内のＭＡＣ
アドレスとＫｓの対応表の
Ｋｓ＿ｅｖｅｎを更新する
S13
データ送信装置は、対象と
する全てのデータ受信装置に
次のＫｓ＿ｅｖｅｎが設定
されたかを把握する

【図１１】

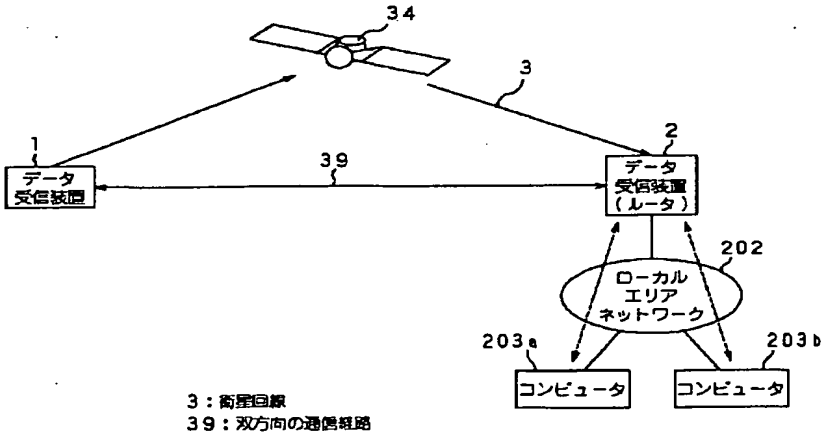



【図１４】

113

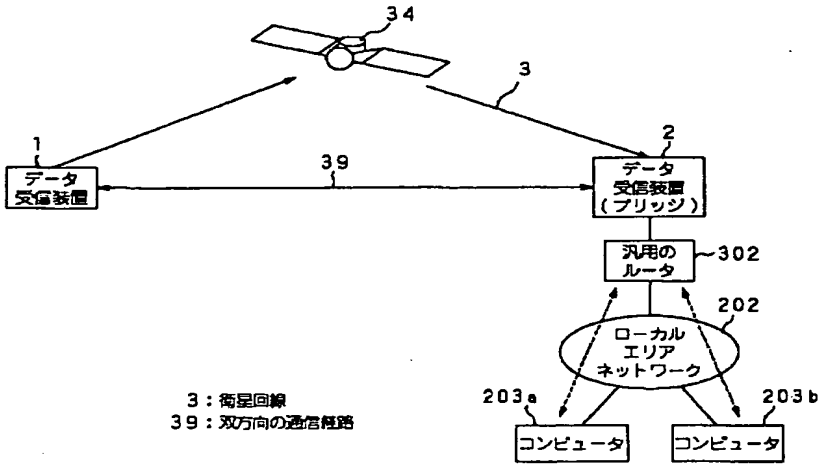
| | | | |
|---|---|---|---|
| VERS | HLEN | SERVIE TYPE | TOTAL LENGTH |
| IDENTIFICAION | | FLAGS | FRAGMENT OFFSET |
| TIME TO LIVE | PROTOCOL | HEADER CHECKSUM | |
| SOURCE IP ADDRESS | | | |
| DESTINATION IP ADDRESS | | | |
| IP OPTIONS(IF ANY) | | | PADDING |
| DATA | | | |
| .... | | | |

【図１５】




3：衛星回線
39：双方向の通信経路

【図１６】


34
3
1
2
39
データ
受信装置
データ
受信装置
（ブリッジ）
汎用の
ルータ
302
202
ローカル
エリア
ネットワーク
203a
203b
コンピュータ
コンピュータ
3：衛星回線
39：双方向の通信経路